

Here are some remarks on the Alice/Bob and premature squeamish ossifrage questions.

The critical document is a thoughtful letter from Richard Schroepel to Ron dated August 1, 1977. The pdf is attached below. Somewhere in my house, I probably have the original photocopy which, I assume Ron gave me, and to which I apparently added:

file under "Schroepel

With regard to Alice and Bob:

On the last page of the document, you'll find:

good symbol for pq, and enter the public exponent, perhaps s. Another literary suggestion: name your protagonists, perhaps Adolf and Bertholt or somesuch. This would reserve isolated letters for mathematical quantities.

I'll add my own recollections. I liked Schroepel's idea, and so did Ron, but he chose Alice and Bob instead of Adolph and Bertholt. I was sympathetic to not using Adolph and Bertholt, but thought Alice and Bob lacked gravitas partially because those names reminded me of the names of the characters in the children's book "Jack and Jill."

With respect to the squeamish ossifrage question:

My current estimate of the time required to factor F8 is 10000 hours of computer time (on a KA10). This makes the constant in my timing formula 2.4 microseconds. Plugging in $N=10^{128}$, I get a time of 50000 years. Of course there are faster computers than the KA10, perhaps by a factor of 300. And the technology keeps getting better. But your number should be safe for many years. The estimated time for my method to factor variously sized numbers on a KA10:

	50	256	100	128	512
N	10	2	10	10	2
$\sqrt{\log N \log \log N}$	10	13	15	17	19
e	1.4×10^4	1.5×10^4	2.3×10^4	6.0×10^4	6.7×10^4
KA10 time	10 hr	1.2 yr	180 yr	50000 yr	5 Myr

A quick calculation with various estimates shows that about 5000 yr of KA10 time was used by Arjen Lenstra's team to factor the challenge and show us the bird. So, it seems that we should have been more careful and listened to Richard's advice.